September 16, 2019

The Honorable Max Rose Chairman, Subcommittee on Intelligence and Counterterrorism 529 Longworth HOB Washington, DC 20515

Dear Chairman Rose:

Thank you for your letter dated September 13, 2019 regarding 8Chan, and for your collaboration in the fight against terrorist and violent extremist use of digital platforms. We appreciate your willingness to work with industry to make the web safer. Please know that Facebook is blocking links to places on 8chan and 4chan that are dedicated to the distribution of vile content.

In addition, we are making a series of organizational, policy and operational shifts that improve how we combat terrorists, violent extremist groups and hate organizations on Facebook and Instagram. We are restricting who can use Facebook Live and have met with world leaders in Paris to sign the New Zealand Government's <u>Christchurch Call to Action</u>. We also co-developed a <u>nine-point industry plan</u> in partnership with Microsoft, Twitter, Google and Amazon, which outlines the steps we're taking to address the abuse of technology to spread terrorist content.

We are expanding the use of automated techniques that we use to identify and surface terrorist content to a wider range of Dangerous Organizations, including both terrorist groups and hate organizations. At Facebook, we've banned more than 200 white supremacist organizations from our platform and we now use a combination of AI and human expertise to remove content praising or supporting these organizations. Our detection techniques include content matching, which allows us to identify copies of known bad material, and machine-learning classifiers capable of identifying a wide range of factors on a post and assessing whether it is likely to violate our policies. This has led to the removal of more than 26 million pieces of content related global terrorist groups like ISIS and al-Qaeda in the last two years, 99% of which we proactively identified and removed before anyone reported it to us.

These efforts are not static. Techniques that are effective against one organization will not always be effective against another and the adversarial nature of counterterrorism work online means that bad actors are often trying to get around our systems. Following the attack in Christchurch, we identified several areas where we needed to improve our ability to detect, review and remove content that violates our policies. At the time, the video depicting the attack in Christchurch did not prompt our automatic detection systems because we did not have enough training data of this specific kind of content since these events are thankfully rare. That's why we're grateful to begin working with government and law enforcement in the US



Address:

and UK to obtain camera footage from their programs. With this initiative, we aim to train our detection systems to recognize real-world, first-person footage of violent events and avoid incorrectly detecting other types of footage such as fictional video games. We'll need to continue to iterate on our tactics because we know bad actors will continue to change theirs, but we think these are important steps and we are excited to work with leaders like you to expand on the proactive detection work in the future.

Again, Thank you for your dedication to this important issue. We stand ready to work with you to combat extremism on the Internet.

Sincerely,

Kevin Martin

Vice President, U.S. Public Policy